
	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:1 DE 24



M-407-01

**POLÍTICAS DE SEGURIDAD
INFORMÁTICA**

ELABORADO POR	REVISADO POR	APROBADO POR
LIDER DEL PROCESO	REPRESENTANTE DE LA DIRECCIÓN	GERENTE GENERAL

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:2 DE 24

I - INTRODUCCIÓN

Hoy es imposible hablar de un sistema cien por ciento seguro, sencillamente porque el costo de la seguridad total es muy alto y no se certifica la seguridad total. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".


La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI) de INFITULUA, surgen como una herramienta organizacional para concientizar a cada uno de los funcionarios sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten al Instituto desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Está lejos la intención (y del alcance del presente) proponer un documento estableciendo lo que debe hacer un usuario o una organización para lograr la mayor Seguridad Informática posible. Sí está dentro de los objetivos proponer los lineamientos generales que se deben seguir para lograr (si así se pretendiese) un documento con estas características.


	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:3 DE 24

El presente es el resultado de la investigación, viendo como muchos documentos son ignorados por contener planes y políticas difíciles de lograr, o peor aún, de entender.

Esto adquiere mayor importancia aun cuando el tema abordado por estas políticas es la Seguridad Informática. Extensos manuales explicando cómo debe protegerse una computadora o una red con un Firewall, un programa antivirus o un monitor de sucesos.

Se intenta dejar en claro que la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.


En palabras de Julio C. Ardita: "Una política de seguridad funciona muy bien en EE.UU. pero cuando estos manuales se trajeron a América Latina fue un fiasco... Armar una política de procedimientos de seguridad en una empresa está costando entre 150-350 mil dólares y el resultado es ninguno... Es un manual que llevado a la implementación nunca se realiza... Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real: las políticas y procedimientos por un lado y la parte física por otra."

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:4 DE 24

II - DEFINICIONES

Para continuar, hará falta definir algunos conceptos aplicados en la definición de una PSI:

- Decisión: elección de un curso de acción determinado entre varios posibles.
- Plan: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.
- Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.
- Política: definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.
- Meta: objetivo cuantificado a valores predeterminados.
- Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.
- Norma: forma en que realiza un procedimiento o proceso.
- Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.
- Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.
- Pronostico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.
- Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.
- Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.


	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:5 DE 24

LOS SIGUIENTES TERMINOS Y DEFINICIONES FUERON TOMADOS DE LA NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC-27001

- Aceptación del riesgo: Decisión de asumir un riesgo.
- Activo: Cualquier cosa que tiene un valor para la organización.
- Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- Confidencialidad: Propiedad de determinar que la información no este disponible ni sea revelada a individuos, entidades ó procesos no autorizados.
- Declaración de aplicabilidad: Documento que describe los objetos de control y los controles pertinentes y aplicables para un Sistema de Control de la Seguridad de la Información.

NOTA Los objetivos de control y los controles se basan en los resultados y conclusiones de los procesos de valoración y tratamiento de riesgos, requisitos legales o reglamentarios, obligaciones contractuales y los requisitos del negocio de la organización en cuanto a la seguridad de la información.

- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgos dados, para determinar la importancia del riesgo.
- Evento de seguridad de la información: Precisa identificar de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:6 DE 24

- Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a seguridad de la información.
- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.
- Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad.
- Sistema de gestión de la seguridad de la información SCS: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar. Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.


NOTA El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

- Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

NOTA En la presente norma el término "control" se usa como sinónimo de "medida".

- Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Ahora, "una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:7 DE 24


Se define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán."

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas." y debe:

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los siguientes elementos claves de seguridad: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los funcionarios. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
	CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017


III – EL RIESGO


La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Algunas veces, el manejo de riesgos se centra en la contención de riesgo por causas físicas o legales (por ejemplo, desastres naturales o incendios, accidentes, muerte o demandas


El objetivo de la gestión de riesgos es reducir diferentes riesgos relativos a un ámbito preseleccionado a un nivel aceptado por la sociedad. Puede referirse a numerosos tipos de amenazas causadas por el medio ambiente, la tecnología, los seres humanos, las organizaciones y la política. Por otro lado, involucra todos los recursos disponibles por los seres humanos o, en particular, por una entidad de manejo de riesgos

3.1 MAPA DE RIESGOS – GESTIÓN INFORMÁTICA - INIFITULUA

		MAPA DE RIESGOS					
Código: F-201-10		Versión: 01		Fecha de aprobación: 29 / ENE / 2010		Página 1 de 1	
PROCESO:		GESTIÓN INFORMÁTICA		OBJETIVO:		Gestionar, administrar y mantener los recursos informáticos y tecnológicos	
ITEM	Factor o Descripción del Riesgo.	Impacto	probabilidad	Evaluación del riesgo	Controles existentes	Valoración del riesgo	Opciones de manejo
1	Daños en los sistemas de información por virus	3	2	M Zona de riesgo moderado	1. Antivirus actualizados 2. Licencias de antivirus actualizadas 3. Divulgación y aplicación de las políticas en materia de seguridad de la información 4. Servidor Proxy para el control del acceso a páginas y aplicaciones no autorizadas de Internet	M Zona de riesgo moderada	Asumir el riesgo
2	Decrecimiento o disminución intensa de la interconexión de la red de datos del instituto	2	1	B Zona de riesgo baja	1. Mantenimiento de la infraestructura de comunicaciones 2. Respaldo (UPS) frente a la interrupción de suministro de energía eléctrica 3. Divulgación y aplicación de las políticas en materia de seguridad y conexión de redes.	B Zona de riesgo baja	Asumir el riesgo
3	Defectos en los componentes físicos y/o de programas de un sistema informático	2	1	B Zona de riesgo baja	1. Mantenimiento de la infraestructura de hardware y software 2. Seguimiento al estado del hardware, Software y su actualización	B Zona de riesgo baja	Asumir el riesgo
4	Incumplimientos en los Acuerdos referentes a los niveles de servicio medidos en los tiempos de respuesta a los usuarios	2	1	B Zona de riesgo baja	1. Cronograma de actividades acordado con los proveedores de Software 2. Comunicación y coordinación con la persona encargada de atender los requerimientos de cada uno de los funcionarios	B Zona de riesgo baja	Asumir el riesgo
5	La infraestructura tecnológica no se encuentra actualizada	2	1	B Zona de riesgo baja	1. Presupuesto fijado para la actual vigencia fiscal 2. Actualización en los normativos y administrativos 3. Estandarización de versiones en los programas y en los equipos	B Zona de riesgo baja	Asumir el riesgo
6	No contar con las debidas licencias de los software instalados en los equipos de la Entidad	3	2	M Zona de riesgo moderado	Seguimiento y/o control por parte de sistemas, Presupuesto fijado para la actual vigencia fiscal	M Zona de riesgo moderada	Reducir el riesgo
7	Perdida de información	4	2	A Zona de riesgo alto	1. Servidor de backups 2. Backups en otro tipo de medios (CD, Memorias USB)	A Zona de riesgo alto	Reducir el riesgo

 Instituto de Financiamiento, Promoción y Desarrollo de Tuluá	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
	CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017

3.2 ADMINISTRACIÓN DEL RIESGO - INFITULUA


		ADMINISTRACIÓN DEL RIESGO		
Código: F-201-11	Versión: 01	Fecha de aprobación: 29 / ENE / 2010	Página 1 de 1	
PROCESO:	GESTIÓN INFORMÁTICA			
RIESGO	RESPONSABLES	ACCIONES	CRONOGRAMA	INDICADOR
Daños en los sistemas de información	Técnico Administrativo	Revisar el control del directorio activo	Semestral	Un directorio activo actualizado
Decrecimiento o disminución intensa de la interconexión de la red de datos del instituto	Técnico Administrativo	Mantenimiento y mejoramiento de la red 6.0	Semestral	Una red instalada.
Defectos en los componentes físicos y/o de programas de un sistema informático	Técnico Administrativo	Mantenimiento de los sistemas de información	Semestral	Seguimiento a cronograma de mantenimiento
Incumplimientos en los Acuerdos referentes a los niveles de servicio medidos en los tiempos de respuesta a los usuarios	Técnico Administrativo	Dar respuesta a requerimientos oportuna	Mensual	No. de soportes atendidos / No. de soportes solicitados
La infraestructura tecnológica no se encuentra actualizada	Técnico Administrativo	Adquisición de licencias de software ofimático actualizado	Anual	No. Licencias adquiridas / No. Licencias Solicitadas
No contar con las debidas licencias de los software instalados en los equipos de la Entidad	Técnico Administrativo	Controlar el vencimiento de las licencias a través de una base de datos la cual será controlada mediante alertas tempranas	Anual	Licencias vencidas / Total de licencias
Pérdida de información	Técnico Administrativo	Back UPS en un servidor web	Mensual	Back UPS realizados / Back UPS programados

IV POLÍTICAS

4.1 APLICACIÓN

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la UNIDAD ADMINISTRATIVA DE SISTEMAS, nombre asignado al Área de Sistemas del Instituto de Financiamiento Promoción y Desarrollo de Tuluá – INFITULUA.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de INFITULUA. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por la Unidad Administrativa de Sistemas, al personal, al manejo de los datos, al uso de los bienes informáticos tanto de

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:10 DE 24

hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

El objetivo principal de la Unidad Administrativa de Sistemas es administrar y mantener los recursos informáticos y tecnológicos de INFITULUA; es brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan, esto es, que tengamos continuidad en el servicio los 365 días del año confiable. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el Instituto son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.


La Unidad Administrativa de Sistemas actualmente está conformado por un (1) funcionario (Técnico Administrativo de Sistemas), el cual cumple distintas funciones referentes a el soporte y mantenimiento de la plataforma tecnológica, desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de la red; dado a esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos

4.2 EVALUACIÓN DE LAS POLÍTICAS

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

4.3 BENEFICIOS

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en la Institución.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:11 DE 24

V. SEGURIDAD INSTITUCIONAL

5.1 POLÍTICA:

Toda persona que ingresa como usuario nuevo a INFITULUA, para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

5.1.1 USUARIOS NUEVOS

Todo el personal nuevo de la Institución, deberá ser notificado a la Unidad Administrativa de Sistemas, con el formato F-403-02 NOVEDADES DE PERSONAL, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

5.1.2 OBLIGACIONES DE LOS USUARIOS


Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

5.1.3 CAPACITACIÓN EN SEGURIDAD INFORMÁTICA

Todo servidor o funcionario nuevo en INFITULUA deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

5.1.4 SANCIONES

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial, o de que se le declare culpable de un delito informático.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:12 DE 24

VI. SEGURIDAD FÍSICA Y MEDIO AMBIENTE

6.1 PROTECCIÓN DE LA INFORMACIÓN Y BIENES INFORMÁTICOS

Para el acceso a los sitios y áreas restringidas se debe notificar a la Unidad Administrativa de Sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

6.1.1.REPORTE DE RIESGO

El usuario o funcionario deberán reportar de forma inmediata a la Unidad Administrativa de Sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

6.1.2 UNIDADES DE ALMACENAMIENTO

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

6.1.3 FUGA DE INFORMACIÓN

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.


6.2 CONTROLES DE ACCESO FÍSICO

6.2.1 ENTRADA Y SALIDA DE EQUIPOS PARTICULARES

Cualquier persona que tenga acceso a las instalaciones de INFITULUA, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en Recepción, en el momento de retirar el equipo de las Instalaciones de INFITULUA, deberá reportar la novedad nuevamente a Recepción, quien revisará en sus archivos el momento de entrada y registrará el momento de salida del activo, también dará un visto bueno de salida.

6.2.2 ENTRADA Y SALIDA DE EQUIPOS DE LA ENTIDAD.

Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información perteneciente a INFITULUA, siempre debe entrar primero al área de inventarios, donde se registrará en el Software Contable, después será asignado

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:13 DE 24

a algún funcionario dependiendo de la necesidad, podrá ser retirado de las instalaciones de INFITULUA,. Se debe diligenciar el formato F-405-04 . con sus respectivas firmas.

6.3 SEGURIDAD EN UNIDADES ADMINISTRATIVAS

Las Unidades Administrativas que componen a INFITULUA, son áreas restringidas, por lo que solo el personal responsable de su Unidad ó el personal autorizado por la Unidad Administrativa de Sistemas (solo para tareas de prevención o correctivo) puede acceder a los diferentes equipos de cómputo.

6.4 PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

6.4.1 TRASLADOS DE EQUIPOS

Los funcionarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Unidad Administrativa de Sistemas, en caso de requerir este servicio, deberá solicitarlo.

6.4.2 RESPONSABILIDAD DEL HARDWARE


El Auxiliar Administrativo de Inventarios de activos será el encargado de generar el resguardo y recabar la firma del funcionario a quien se le asigne un equipo de cómputo, como responsable de los activos informáticos que se le establezcan y de conservarlos en la ubicación autorizada por la Unidad Administrativa de Sistemas.

6.4.3 RESPONSABILIDAD DE LA FUNCIÓN DEL EQUIPO

INFITULUA, será quien ponga a disposición de los usuarios los medios y equipos informáticos para el cumplimiento de sus obligaciones laborales. En consecuencia, dichos equipos informáticos no están destinados al uso personal o extra profesional de los usuarios, por tanto, estos deben de conocer que no gozan del uso privativos de los mismos.

6.4.4 CAPACITACIÓN DE HERRAMIENTAS INFORMÁTICAS

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:14 DE 24

6.4.5 GUARDAR INFORMACIÓN

Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro c:\Mis Documentos, es responsabilidad del Técnico Administrativo en Sistemas re direccionar esta carpeta al servidor principal.

6.4.6 RECOMENDACIÓN DE NO INGERIR BEBIDAS O COMIDA CERCA A LOS EQUIPOS INFORMÁTICOS

Mientras se esté cerca a el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

6.4.7 RECOMENDACIÓN DE NO COLOCAR OBJETOS SOBRE LOS EQUIPOS DE CÓMPUTO.

Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

6.4.8 CONDICIONES AMBIENTALES PARA EL EQUIPO DE CÓMPUTO

Se debe mantener el equipo informático en un lugar limpio y sin humedad.

6.4.9 CABLES DE CONEXIÓN

El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal de la Unidad Administrativa de Sistemas

6.4.10 ABSTENCIÓN DE ABRIR LOS EQUIPOS DE COMPUTO


Queda terminantemente prohibido que el usuario o funcionario distinto al personal de la Unidad Administrativa de Sistemas abra o destape los equipos de cómputo. No se podrá acceder físicamente al interior de los PC's.

6.5 MANTENIMIENTO DE EQUIPOS

Únicamente el personal autorizado por la Unidad Administrativa de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

6.5.1 RESPALDO DE INFORMACIÓN SENSIBLE

Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:15 DE 24

se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

6.5.2 PRESTAMO DE EQUIPOS INFORMÁTICOS

El funcionario que solicite el préstamo de un equipo informático debe llenar el formato F-405-04 ENTRADA Y SALIDA DE ACTIVOS, con la respectiva firma del Auxiliar Administrativo de Inventarios e informar a su superior.

6.5.3 PERDIDA, ROBO O EXTRAVIO DE EQUIPOS DE CÓMPUTO.

El servidor o funcionario deberán dar aviso inmediato a su superior, la Unidad Administrativa de Sistemas y al Auxiliar Administrativo de Inventarios de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

6.6 USO DE DISPOSITIVOS EXTRAIBLES

A excepción de los administrativos de INFITULUA y la Unidad Administrativa de Sistemas queda prohibido el uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de CD y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.


Si algún funcionario necesita realizar una copia debe comunicarlo a la Unidad Administrativa de Sistemas, el Técnico Administrativo de Sistemas realizará el procedimiento de copiar a dispositivos extraíbles.

6.7 DAÑO DEL EQUIPO

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, por descuido o negligencia por parte del usuario responsable, se le levantara un reporte de no conformidad formato F-401-06 REPORTE DE NC, AC Y AP, por incumplimiento de políticas de seguridad Informática.

7. ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO.

Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de INFITULUA. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna o redes externas como internet.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:16 DE 24

7.1 PREVENCIÓN DE CODIGO MALICIOSO

Los usuarios y funcionarios de INFITULUA que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

7.2 USO DEL ANTIVIRUS

Regularmente el Técnico Administrativo de Sistemas debe actualizar los antivirus y capacitar a los funcionarios en el uso básico de esta herramienta.

7.3 ENTRADA AL CENTRO DE COMPUTO DE SERVIDORES

Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar a la Sala donde se encuentren los Servidores, debe comunicarlo a la Unidad Administrativa de Sistemas, especificando el tipo de actividad a realizar, firmar la bitácora de visitas y siempre contar con la presencia del Técnico Administrativo de Sistemas.

7.4 REGISTRO DE VISITANTES A CENTRO DE COMPUTO

El Técnico Administrativo de Sistemas debe llevar un registro de visitantes del centro de cómputo.

7.5 MANTENIMIENTO DE EQUIPOS SERVIDORES

Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido (servidores), se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

8. ADQUISICIÓN DE SOFTWARE


Los funcionarios de INFITULUA, deben hacer uso exclusivo de las aplicaciones informáticas o versiones de software instalado en los equipos de cómputo.

8.1 SOLICITUD DE SOFTWARE

Los usuarios y funcionarios que requieran la instalación de software que sea propiedad de INFITULUA, deberán justificar su uso y solicitar su autorización llenando el formato F-407-06 SOLICITUD DE ACCESO, con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

8.2 RESTRICCIÓN DE INSTALACIÓN DE SOFTWARE

Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de INFITULUA. El

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:17 DE 24

único personal autorizado para instalar software es el Técnico Administrativo de Sistemas.

8.3 CAPACITACIÓN SOBRE EL USO DE SOFTWARE LEGAL

La Unidad Administrativa de Sistemas, tiene a su cargo la tarea de informar periódicamente a la comunidad de INFITULUA, Directivos, Administrativos Técnicos, Auxiliares, su política institucional contra la piratería de software, utilizando todos los medios de comunicación disponibles: Página intranet, Emails, Carteleras y Boletines.

8.4 COMPRA Y USO EXCLUSIVO DE SOFTWARE LEGAL

El Instituto DE Financiamiento, Promoción y Desarrollo de Tuluá – INFITULUA, tiene como política comprar los equipos de cómputos debidamente licenciados con el sistema operativo y el software ofimático de Microsoft, necesario para el buen desempeño de las labores de los funcionarios. Esto nos garantiza en gran medida la legalidad de los programas adquiridos. Cualquier otro "software" requerido, y que no pueda ser provisto por la compañía Microsoft, será adquirido a otro Proveedor debidamente certificado, el cual deberá entregar al momento de la compra, el programa y la licencia del software con toda la documentación pertinente y necesaria que certifique la originalidad y validez del mismo.

8.5 RESGUARDO DE MEDIOS, CD'S DE SOFTWARE LEGAL


El control de manejo para las licencias y el inventario de los Medios, paquete de CD's será responsabilidad del Auxiliar Administrativo encargado de los inventarios de INFITULUA.

8.6 REINSTALACIÓN DE SOFTWARE

En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

8.7 CARPETA DONDE SE RELACIONA LAS LICENCIAS DE SOFTWARE PROPIEDAD DE INFITULUA

Es obligación del Técnico Administrativo de Sistemas llevar la carpeta 400-30-1 INVENTARIO DE LICENCIAS DE SOFTWARE. Debidamente diligenciada y al día.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:18 DE 24

9. IDENTIFICACIÓN DE INCIDENTES

Los funcionarios de INFITULUA, están obligados a notificar cualquier incidencia o anomalía en el uso de medios informáticos que detecten: pérdida de información, de listados, accesos no autorizados, uso de su identificador de usuario ó de su contraseña, introducción de virus, recuperación de datos, desaparición de soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.

9.1 OBLIGACIÓN DEL FUNCIONARIO

El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo a la UNIDAD Administrativa de Sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

9.2 DE LA INFORMACIÓN CONFIDENCIAL

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar a la Dirección Financiera y Administrativa de INFITULUA.

9.3 INCIDENTES CON ACTIVOS TÉCNOLÓGICOS

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de INFITULUA, debe ser reportado a la Unidad Administrativa de Sistemas.

9.4 BASE DE CONOCIMIENTO - CONTRO DE INCIDENTES


Es obligación del Técnico Administrativo llevar un libro de control de incidentes.

10. ADMINISTRACIÓN DE LA RED

Los funcionarios de INFITULUA no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización de la Unidad Administrativa de Sistemas.

10.1 SEGURIDAD PARA LA RED

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por Unidad Administrativa de Sistemas, en la cual los usuarios o funcionarios realicen la exploración de

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:19 DE 24

los recursos informáticos en la red de INFITULUA, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

10.2 SEGURIDAD DE CONEXIÓN

Queda prohibido comunicarse a la red corporativa de INFITULUA por otros medios distintos a los definidos y administrados por el Instituto.

10.3 DE LOS EQUIPOS DE COMPUTO

Queda prohibido conectarse a la red corporativa con cualquier equipo informático distinto a los instalados por INFITULUA. El personal externo solo tiene acceso a internet por medio de la tecnología Wi – Fi. Si en algún momento se requiere que personal externo se conecte a la red corporativa requiere de autorización y supervisión permanente del Técnico Administrativo de Sistemas.

10.4 USO DE USUARIO Y CONTRASEÑA

Todo funcionario que use los activos informáticos de INFITULUA, debe tener un usuario y contraseña, personal e intransferible, la contraseña debe cumplir con controles de seguridad como: Mínimo 8 caracteres, debe contener letras mayúsculas, letras minúsculas, números y caracteres especiales.

10.5 CUSTODIA DE IDENTIFICACIÓN DE USUARIO Y CONTRASEÑA


Los funcionarios deben custodiar convenientemente su identificación de usuario y/o contraseña, sin proceder a su revelación o puesta al alcance de terceros, serán responsables de toda actividad relacionada con el uso de su acceso personal autorizado.

10.6 PERIODICIDAD DE LA CONTRASEÑA

Las contraseñas tendrán una vigencia de 30 días, por lo tanto los funcionarios deben proceder a cambiarlas siguiendo las instrucciones del Técnico Administrativo de Sistemas.

10.7 RESTRICCIÓN DE ACCESO NO AUTORIZADO

Los funcionarios no deben intentar obtener otros derechos de acceso diferentes a los asignados por la Unidad Administrativa de Sistemas, ni utilizar otro acceso autorizado que corresponda a otro usuario.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:20 DE 24

11 ACCESO A INTERNET

El acceso a Internet provisto a los funcionarios de INFITULUÁ es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

11.1 ACCESO A INTERNET

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos INFITULUA, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por la Unidad Administrativa de Sistemas.

11.2 REPORTES DE INCIDENTES CON INTERNET

Los usuarios de Internet de INFITULUA tienen que reportar todos los incidentes de seguridad informática a la Unidad Administrativa de Sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática generado desde internet.

11.3 ACUERDOS DE USO DE INTERNET

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

11.3.1 Serán sujetos de monitoreo de las actividades que realiza en Internet.


11.3.2 Saben que existe la prohibición al acceso de páginas no autorizadas.

11.3.3 Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

11.3.4 Saben que existe la prohibición de descarga de software sin la autorización de la Unidad Administrativa de Sistemas.

11.3.5 La utilización de Internet es para el desempeño de sus funciones y cargo en INFITULUA y no para propósitos personales.

11.3.6 Las autorizaciones de acceso a internet se concederán acordes con las funciones del puesto que desempeñe el funcionario, produciéndose una segmentación de perfiles que habiliten las conexiones. En INFITULUA, los funcionarios que utilizan internet están clasificados en 5 grupos, a saber:

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:21 DE 24

- **ACCESO DENEGADO:** Para funcionarios que por funciones de su labor no necesitan del servicio de internet.
- **ACCESO GREEN** Para funcionarios que solo deben entrar a pocas paginas de internet, tales como: correo electrónico, talk Skype, paginas gubernamentales (terminación .gov.co).
- **ACCESO CONTABLE** Para funcionarios del área de contabilidad y tesorería, que fuera del Acceso Green necesitan por su trabajo visitar o consultar otras fuentes del ámbito contable y jurídico.
- **ACCESO BLUE:** Es para todos los usuarios y visitantes que necesitan de internet por medio de WII FI.
- **ACCESO UNFILTERED** para funcionarios que por necesidades de su labor necesitan de libre tráfico en internet.

Es importante mencionar que está prohibido entrar a dominios tales como; Facebook, live, Hotmail, msn u otros dominios de mensajería diferentes al institucional.

11.3.7 Queda terminantemente prohibido la instalación de proxys por los usuarios.


11.3.8 La transferencia de datos desde o a internet se realizara exclusivamente cuando lo exija el ejercicio de las funciones del puesto de trabajo. En todo caso, los usuarios deberán tener en cuenta, antes de utilizar la información proveniente de la red, si dicho uso es conforme a las normas que protegen la propiedad intelectual e industrial.

12. CORREO ELECTRÓNICO.

INFITULUA suministrara a cada usuario una dirección individual de correo electrónico, procediendo a instalar y configurar una cuenta de correo. El acceso a dicha cuenta de correo se efectuará mediante una clave personal.

12.1 los usuarios tienen prohibido terminantemente el uso en las redes de comunicaciones propiedad del Instituto, de otras cuentas de correo electrónico distintas a las facilitadas por INFITULUA.

12.2 El uso por los funcionarios del correo electrónico habilitado por INFITULUA es estrictamente profesional, es decir, para el ejercicio de las funciones que corresponden al puesto de trabajo que desempeñe.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:22 DE 24

12.3 los usuarios no pueden interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otros usuarios.

12.4 Está prohibido el uso abusivo del correo electrónico, utilizando mensajes con contenidos ofensivos o atentatorios a la dignidad humana, así mismo, queda prohibido el envío deliberado de cualquier clase de programa o virus que puedan causar perjuicios en los sistemas de información de INFITULUA o a terceros.

12.5 con la finalización de la relación funcional o laboral se interrumpirá el acceso a la cuenta de correo del usuario por parte de la Unidad Administrativa de Sistemas.

12. ACCESO LÓGICO A LA INFRAESTRUCTURA RED LAN

Cada funcionario ES responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, de su “ I D ” login de usuario y contraseña necesarios para acceder a la red interna de información (red LAN) y a la infraestructura tecnológica de INFITULUA, por lo que se deberá mantener de forma confidencial.

12.1 RESPONSABILIDADES DEL ACCESO LOGICO

Todos los usuarios de servicios de información son responsables por el ID de usuario y contraseña que recibe para el uso y acceso de los recursos.


12.1.1 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de INFITULUA, a menos que se tenga el visto de su jefe inmediato y la Unidad Administrativa de Sistemas.

12.1.2 Cada usuario que acceda a la infraestructura tecnológica de INFITULUA debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

12.1.3 Los funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

12.2 ADMINISTRACIÓN DE PRIVILEGIOS

Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la Unidad Administrativa de Sistemas, para el cambio de

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:23 DE 24

privilegios, mediante el formato F-407-06 SOLICITUS DE ACCESO. Y el formato F-403-02 NOVEDADES DE PERSONAL

12.3 DIRECTIVAS DE GRUPO

Por política de seguridad informática todos los equipos de cómputo de INFITULUA, están conectados a un servidor principal que administra el Active Directory por lo tanto cumple con algunas directivas de grupo ó GPO.

Todos los equipos de cómputo de INFITULUA, están divididos en 4 unidades administrativas dentro del Active Directory que son:

- ADMINISTRADORES: Donde se ubican todos los usuarios que tienen permiso de administración de la red LAN
- DIRECTORES: Donde se ubican todos los usuarios que son de tipo administrativo para INFITULUA.
- TERMINAL SADMIN: Donde se ubican todos los usuarios que interactúan con el software integral SADMIN.
- USUARIOS OFICINA: Donde se ubican todos los usuarios que solo utilizan las políticas y GPO generales del servidor.


Las directivas de grupo existentes en INFITULUA son:

- ACTUALIZACIONES VARIAS
- DEFAULT DOMAIN POLICY
- DEFAULT DOMAIN CONTROLLERS POLICY
- GPO USUARIO DESATENDIDO
- GPO TERMINAL SERVER

Dependiendo de las características de las unidades administrativas, se aplican una o varias GPO.

12.4 ACCESO REMOTO POR INTERNET

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización de un directivo de INFITULUA y con un mecanismo de control de acceso seguro autorizado por la Unidad Administrativa de sistemas.

	MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA		
CODIGO: M-407-01	VERSIÓN: 03	FECHA: 22/12/2017	PAGINA:24 DE 24

13. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La Unidad Administrativa de Sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

14. DERECHOS DE PROPIEDAD INTELECTUAL

Los sistemas desarrollados por personal interno o externo que controle la Unidad Administrativa de Sistemas son propiedad intelectual de INFITULUA.

15. CLAUSULA DE CUMPLIMIENTO

La Unidad Administrativa de Sistemas realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

La Unidad Administrativa de Sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportados ante la Directora Financiera y Administrativa.

16. VIOLACIONES DE SEGURIDAD

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

16.1 Ningún usuario o funcionario de INFITULUA debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la Unidad Administrativa de Sistemas.

16.2 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de INFITULUA.

17. SOBRE EL CONOCIMIENTO DE LAS INSTRUCCIONES

Todos los usuarios de los sistemas de información y redes de comunicaciones que sean propiedad o que estén bajo la supervisión de INFITULUA, están obligados al conocimiento y cumplimiento de las presentes instrucciones.